DOI: http://dx.doi.org/10.5235/17579961.6.2.147 (2014) 6(2) LIT 147–167

The Law as a 'Catalyst and Facilitator' for Trust in E-Health: Challenges and Opportunities

Anton Vedder, Colette Cuijpers, Petroula Vantsiouri and Mariana Zuleta Ferrari*

I. INTRODUCTION

In 2012, the World Health Organization (WHO) published a report on the state of development of legal frameworks with regard to e-health.[1] The report is based on the findings of the WHO's Second Global Survey on E-Health, which analysed, amongst other things, the extent to which the legal frameworks in the Member States addressed the need to protect patients' privacy in the use of electronic healthcare applications. Based on the results obtained, the WHO stressed the fact that although in most member countries there exists a high level of legal protection of the general privacy of health-related information, this does not go beyond the common human right of privacy. There exists little specific e-health related privacy protection legislation and much remains to be explored in terms of other legal safeguards.

This article intends to broaden the WHO's analysis and go somewhat further, exploring not only the challenges and opportunities with regard to privacy protection, but also liability laws, which could have a significant impact on the use and adoption of these technology applications.[2]

II. PRELIMINARIES

In the years to come, ageing and the diminution of labour potential are expected to strain existing care systems gradually, to the extent that maintaining current levels of

* Anton Vedder, ICRI-CIR, KU Leuven and TILT, Tilburg University; Colette Cuijpers, Petroula Vantsiouri and Mariana Zuleta Ferrari, TILT, Tilburg University, The Netherlands. All websites accessed November 2014.

1 World Health Organization, *Legal Frameworks for eHealth, based on the findings of the second global survey on eHealth* (Global Observatory for eHealth series, vol 5, 2010, WHO Survey on eHealth), 6, http://whqlibdoc.who.int/publications/2012/9789241503143_eng.pdf.

2 The research presented in this article was carried out in the context of the THeCS project, which is funded by COMMIT.

healthcare provision will become difficult.[3] Many experts believe that electronic healthcare applications will assist in overcoming those difficulties by providing treatment and care to patients in a variety of subdomains of the care system in a safe and efficient manner. Of course, e-health can only successfully contribute to a sustainable healthcare system when care providers and patients effectively accept and adopt those applications.

For briefness' sake we will refer to the applications as e-health. The European Commission uses e-health as the overarching term for the range of tools based on information and communication technologies used to assist and enhance the prevention, diagnosis, treatment, monitoring and management of health and lifestyle.[4] Many expect e-health to gradually replace certain traditional methods of healthcare provision and treatments for intrinsic qualitative reasons, and for its expected contribution to the sustainability of the healthcare system.[5] E-health is often advocated as a less labour intensive and more cost effective method of delivering healthcare than traditional practices. Many researchers and policy makers see in e-health the opportunity to promote the improvement of healthcare quality while reducing, instead of increasing, the current levels of resources spent on care.[6]

In this article, we will for the sake of the argument assume that the efficacy, efficiency and safety evaluations remain promising. We are well aware that a lot of evaluative research still needs to be done. We tend to favour a critical, well-considered stance rather than precocious advocacy. Assuming nonetheless for the time being that from the perspectives of overall efficacy, efficiency and safety, e-health remains a favourable alternative compared to traditional care provision and treatment, an important question is: How should we make the transition from a functioning system of delivery of healthcare to a system where new dynamics and demands take place, creating new scenarios and new positions and relationships? As long as traditional forms of care and e-health alternatives

3 Eurostat forecasts suggest that the proportion of the population aged 65 or over will rise from 17.1% in 2008 to 30% in 2060. The average ratio between people of working age (15–64) and people aged 65 and over will change from 4:1 now to 2:1 in 2050. See Opinion 2011/C44/02 of the European Economic and Social Committee on 'The Impact of Population Ageing on Health and Welfare Systems' (exploratory opinion).

4 Definition offered by DG Health and Consumers, European Commission, http://ec.europa.eu/health/ehealth/policy/index_en.htm.

5 AG Ekeland, A Bowes and S Flottorp, 'Effectiveness of Telemedicine: A Systematic Review of Reviews' (2011) 79 *International Journal of Medical Inf*ormation 736; C LaPlante and W Peng, 'A Systematic Review of eHealth Interventions for Physical Activity: An Analysis of Study Design, Intervention Characteristics, and Outcomes' (2011) 17 *Telemedicine and e-Health* 509; J Polisena, K Tran, K Cimon, B Hutton *et al*, 'Home Telehealth for Chronic Obstructive Pulmonary Disease: A Systematic Review and Meta-Analysis' (2010) 16(3) *Journal of Telemedicine and Telecare* 120; J Pols, *Care at a Distance* (Amsterdam University Press, 2012).

6 Currently the amount of activity involving the management and delivery of health services in the European Union represents 9.6% of the GDP. European Commission, *Joint Report on Health Systems* (Occasional Papers 74-2010), 11, http://ec.europa.eu/economy_finance/publications/occasional_paper/2010/op74_en.htm.

are provided simultaneously—as is currently often the case—patients will need extra incentives to start and keep using e-health instead of continuing to use the traditional facilities they are accustomed to. For this reason, the transition requires preparatory reflection. Users will need to be persuaded by advanced efficacy, efficiency, safety, and ease of use ratios, but also by safeguards against harms and privacy infringements, which do not usually arise in traditional care, but could do so with the new applications due to their electronic infrastructure.

Can law foster trust in e-health, especially during the stage of transition? In what way can the law contribute to the acceptance and adoption of e-health applications? It is in contexts such as this transition stage, in which trust is in the process of being established, or needs to be strengthened or reinforced, that complementary tools to ensure reliable behaviour become relevant.[7]

One way of applying the law for this purpose could consist of the imposition of e-health applications on patients and healthcare providers via the command and control function of law. Legislation could, for example, establish that specific services may be offered only electronically, or the state may require healthcare providers to offer e-health services as part of their practice. Such approaches, however, could face stakeholder resistance, given the diversity of degrees of development and completion of e-health alternatives for the various forms of care and the strongly developed culture of professional autonomy in the healthcare domain. Under this scenario e-health is imposed upon patients and healthcare providers instead of being freely chosen by them for positive reasons. The acceptance of e-health may be fragile and thus negatively impact its contribution to sustainable healthcare.

Some stakeholders in the field of e-health may perceive this command and control function of the law very negatively. For healthcare providers and IT developers, for instance, law may appear *prima facie* as an extra conditionality without much practical use. From an innovator's perspective, law may be perceived as a stumbling block to renewal, as an external factor burdening the conduct of healthcare providers and meddling with the provision of healthcare.

A different approach might be more promising. One can allow the law to play a primarily instrumental role in shaping social behaviour, not as an expression of state command, but rather as a framework that creates the conditions for interactions between state, market and individuals, and delineates the boundaries between them.[8] The legal institutions framing and enforcing relevant obligations enable individuals to trust counterparts to the degree that they are prepared to take the risks accompanying

7 R Hardin, *Trust* (Polity Press, 2006) 103.

8 For the role of law as a threat, proscribing conduct and threatening sanctions for violation to deter that conduct, and the role of law as an umpire, creating and policing boundaries of a space for free and secure interaction between participants, see B Morgan and K Yeung, *An Introduction to Law and Regulation* (Cambridge University Press, 2007) ch 1.

mutual exchanges and interactions, in order to obtain the benefits that are also attached to them.[9] In other words, the law may be able to create necessary conditions for healthcare providers and patients to trust e-health and adopt it voluntarily, instead of being coerced to do so.

Recently the introduction of the care.data scheme—a modern data service from the Health and Social Care Information Centre (HSCIC) for the entire health and social care system—has raised controversies in the United Kingdom.[10] The HSCIC, created by the Health and Social Care Act 2012, collects and shares confidential information contained in medical records (only the names are left out of the records) for purposes of care research and policy making. It has met with strong criticism from individual doctors and the British Medical Association on the basis that the scheme suffers from a lack of awareness (and, hence, lack of legitimacy) on the part of the general public.[11] As a consequence, the roll-out of the record extraction procedures has been severely delayed, thus exemplifying simultaneously the general significance of privacy and confidentiality for user trust and the inadequacy of the one-sided use of the control and command function of law.

Is the law merely an annoying inconvenience, or can it boost reliance on e-health and make law a driving force for e-health in the future? A look at the existing EU and US legal framework on privacy and data protection and liability reveals that, for instance, through the patient's right to privacy, the duty of confidentiality, contract and tort law, and the doctrine of liability, the law already plays an instrumental role in shaping trust in traditional offline healthcare systems. In addition to special laws on a national level regarding the caregiver-patient relationship, (para-)medical professions and care institutions, national and international legal frameworks already offer general starting points that are important for healthcare systems, and have long been doing so.

This article argues that the law can play an important part in the transition from traditional healthcare to the e-health era. To that end, section III examines the changes that e-health brings about with respect to the roles and responsibilities of care providers, system providers and patients, and the impact on user trust that these changes can have. Section IV addresses the issue of user trust in the age of e-health. It should be noted that users of e-health applications are not only patients, but also healthcare providers who rely on e-health applications for the provision of healthcare. Section V explores the ways in which privacy and data protection and liability law can play a role in the adoption of e-health as a response to the changes to the traditional care practices that e-health entails.

9 Hardin (n 7) 88; compare J Raitio, *The Principle of Legal Certainty in EC Law* (Kluwer, 2003).

10 For more information regarding care.data, see www.hscic.gov.uk/article/3525/Caredata. For criticism, see eg www.pifonline.org.uk/criticism-of-nhs-england-care-data-information.

11 For an overview of the debate and BMA's position, see http://bma.org.uk/practical-support-at-work/ethics/confidentiality-and-health-records/care-data.

III. CHANGES

We shall illustrate the relevant changes to traditional healthcare practices by considering one type of e-health application—'remote monitoring and treatment systems'—a little more closely. This application plays a role in the provision of care for the elderly and chronically ill patients by supporting them in developing and maintaining an active lifestyle. These systems can alleviate or halt the deterioration of their health, either independently or supervised remotely by healthcare professionals.[12] They usually integrate ambulant sensing to measure relevant bio signals and context information with secure data handling and appropriate clinical decision support functionality to assist in both technical and clinical decision making.[13] They may also provide feedback to both patients and care providers. So far these e-health systems have focused on the elderly for vital sign monitoring,[14] on patients with various conditions, including obesity, chronic obstructive pulmonary disease (COPD) and chronic fatigue syndrome (CFS),[15] and on cardiac patients.[16] The systems operate based on human–computer interaction through various media, such as television,[17] smartphones[18]and web-based communities.[19]

Remote monitoring and treatment systems provide continuous monitoring of the health status of the patient with (the promise of) opportunities for coaching or continuous motivational help aimed at achieving behavioural change, whenever required, and individually tailored treatment anywhere and anytime. They support greater independ-

12 HJ Hermens and MM Vollebroek-Hutten, 'Towards Remote Monitoring and Remotely Supervised Training' (2008) 18(6) *Journal of Electromyography and Kinesiology* 908.

13 *Ibid*.

14 A Czabke, J Loeschke and TC Lueth, 'Concept and Modular Telemedicine Platform for Measuring of Vital Signs, ADL and Behavioral Patterns of Elderly in Home Settings' [2011] *Architecture* 3164.

15 H op den Akker, VM Jones and HJ Hermens, 'Predicting Feedback Compliance in a Teletreatment Application', paper presented at ISABEL 2010, the 3rd International Symposium on Applied Sciences in Biomedical and Communication Technologies, Rome, Italy 2010.

16 S Kumar, K Kambhatla, F Hu, M Lifson and Y Xiao, 'Ubiquitous Computing for Remote Cardiac Patient Monitoring: A Survey' (2008) IV *International Journal of Telemedicine and Applications* 459185; VM Jones, HJ Hermens, P Leijdekkers and R Rienks, 'Extending Remote Patient Monitoring with Mobile Real Time Clinical Decision Support', paper presented at the Annual Symposium of the IEEE EMBS Benelux Chapter 2009.

17 TM Burkow, LK Vognild, T Krogstad, N Borch, G Ostengen, A Bratvold and MJ Risberg, 'An Easy to Use and Affordable Home-Based Personal eHealth System for Chronic Disease Management based on Free Open Source Software' (2008) 136 *Studies in Health Technology and Informatics* 83.

18 See n 15; W Wieringa, H op den Akker, VM Jones, R op den Akker and HJ Hermens, 'Ontology-Based Generation of Dynamic Feedback on Physical Activity' in *Proceedings of the 13th Conference on Artificial Intelligence in Medicine (AIME)* (Springer, 2011) 55; O Stahl, B Gamback, P Hansen, M Turunen and J Hakulinen, 'A Mobile Fitness Companion' (2008) 59 *Science and Technology* 38; G Chen, B Yan, M Shin, D Kotz and E Berke, 'MPCS: Mobile-Phone Based Patient Compliance System for Chronic Illness Care' [2009] *Mobile and Ubiquitous Systems Networking Services* 1–7.

19 B Lewis *et al*, 'User Attitudes towards Physical Activity Websites in a Randomized Controlled Trial' (2008) 47(5) *Preventive Medicine* 508.

ence and self-management of lifestyle and disorders. Their purpose is to make healthcare more efficient and effective and less costly.

What are the possible consequences and implications with regard to practices of care and the care provider–patient relationship when compared to traditional healthcare methods? First, the use of electronic networks and digital technology allows for continuous monitoring and collection and storage of data that can be used for all kinds of purposes: treatment, extra coaching or motivation, but also evaluation by different stakeholders for various purposes. Second, the medical practice involved in remote monitoring and treatment systems is a service of multiple physicians and other care providers with multiple specialities. The exercises proposed, for instance, by a remote monitoring system to a COPD patient, who is also suffering from cardiac health problems, might stem from a pulmonologist, but may also be reviewed by cardiologists. In contrast to traditional health practices, where the COPD cardiac patient would need to consult two healthcare professionals separately, or—in advanced cases of chain structuring of care provision—simultaneously,[20] within an e-health context, the exchange and access to information regarding the patient is taking place in the absence of the patient and outside her control. In addition, with regard to the feedback received by the patient, it may not always be entirely clear to her whether it is the pulmonologist, the cardiologist or the 'system' that instructs her to exercise and monitors her condition.

Under these circumstances, the patient using a remote monitoring and treatment system must trust not only her multiple physicians, but also the application and the way it communicates the information between herself and the multiple physicians. The situation becomes more complex as care is often provided in integrated delivery systems or coordinated by large institutions.[21] The participating organisations are more often than not of different kinds: public, private or of mixed public-private character, to which different moral expectations and legal regimes apply.

Moreover, the devices and software enabling the provision of e-health services also become tools directly involved in diagnosis and treatment. Remote monitoring and treatment systems will gradually replace the advice that was traditionally provided in person by the healthcare practitioner with daily, often automatically produced, instructions.

Perhaps most significantly, the patient acquires a new role, as she becomes actively involved in her own diagnosis and treatment. She has systematic tasks related to describing her condition, taking measurements or performing exercises and (part of) her own therapy—all of this in the absence of healthcare providers.

20 In traditional healthcare systems the treatment of patients in multimorbid conditions is often designed by healthcare practitioners of different specialities; however, in contrast to e-health services the deliberation often takes place in the presence of the patient.

21 Indicatively see the Condition Coach (CoCo) care service for self-management of physical fitness for COPD or chronic patients administered by the Roessingh Telecare Center, www.roessinghtelezorg.nl/producten-diensten/conditie-coach.html.

In this section, we have described some of the changes that the introduction of electronic applications in the provision of healthcare may bring about on the basis of an illustrative example. The most important relevant changes are:

- the extensive collection and storage of data that can be used for various purposes by different stakeholders, certainly boosting the possibilities of quantification, evaluation and evidence-based medicine;
- the introduction of a plurality of caregivers and technology providers;
- the new roles of and relationships between care providers and patients.

Before we start exploring whether, and if so in what ways, the law may contribute to building trust for patients and providers in services and practices that are relatively new to them, we will take a closer look at trust and e-health services in general.

IV. TRUST

Instead of entering the academic debate on definitions of trust, we will for the purposes of this article and for briefness' sake just propose a stipulative definition of trust as an inclination of human beings to believe that a form of direct or indirect interaction with another person, thing or system may be beneficial to them or at least not harm their interests.[22] Trust defines the relationship between a person that trusts and a trustee, ie the person, group, organisation, animal or thing being trusted.[23] A trustee may simultaneously act as a trustor, and vice versa. For example, a patient, acting as a trustor, has to be certain about the identity of the medical professional, acting as a trustee. Vice versa, the medical professional, who is simultaneously acting as a trustor, has to be certain about the identity of the patient, simultaneously acting as a trustee. (Groups of) people, professions, organisations and whole societies can all be trustors and trustees at the same time.

Many studies on trust have elaborated on the various qualities and dimensions of the trustor, the trustee and their mutual relationship that can be considered to be preconditions of some sort for trust. *Reputation* and *good past performance* of the trustee, for instance, have been deemed to be crucial factors impacting the trustworthiness of the trustee.[24] The introduction of electronic services has made it necessary to pay additional

22 Cf P Dasgupta, 'Economic Progress and the Idea of Social Capital' in P Dasgupta and I Serageldin, *Social Capital: A Multifaceted Perspective* (World Bank, 2000) 330.

23 M Taddeo, 'Modelling Trust in Artificial Agents: A First Step toward the Analysis of e-Trust' (2010) 20(2) *Minds and Machines* 243.

24 P Sztompka, *Trust: A Sociological Theory* (Cambridge University Press, 1999); M Levi, 'Sociology of Trust' in *International Encyclopedia of the Social & Behavioral Sciences* (Elsevier, 2001) 15922–6; L Kool, B van

attention to the notion of trust, since when using them individuals find themselves in situations where they need to rely on technologies, systems, and other actors whom they do not know or cannot see face to face. Reputations and the past performance of relevant parties have often not yet been established.

Trust in e-services requires not only trust in the providers of the services offered, but also trust in the technology involved.[25] This applies *mutatis mutandis* to trust in e-health services as well. Patients' trust in e-health can be subdivided into trust in the healthcare providers and trust in the reliability of the specific system used. To take an example, a patient using a medical device that measures her blood pressure and transfers the resulting data to the physician via the internet should trust not only the physician examining her but also the system that transfers the data. Online environments lack the benefits of offline face-to-face communication and the ability to observe the service provider's behaviour directly. The traditional means of establishing and conferring credibility in terms of reputation and quality of past performance are no longer present, and need to be replaced by new means.

In addition to reputation and past performance, several other factors are relevant to the user in order to trust in electronic services.

An overall positive attitude towards the internet is often identified as a general key predictor of e-service adoption,[26] as is *previous experiences* with a provider of an electronic service.[27]

Schoonhoven, M van Lieshout, A Vedder and FM Fleurke, 'Trusted Technology: Een onderzoek naar de toepassingsvoorwaarden voor Privacy by Design in de electronische dienstverlening van de overhead' (TNO en TILT rapport 35598 in opdracht van Alliantie Vitaal Bestuur 2011) 33; RC Mayer, JH Davis and DF Schoorman, 'An Integrative Model of Organizational Trust' (1995) 20(3) *Academy of Management Review* 709; TK Das and BS Teng, 'The Risk-Based View of Trust: A Conceptual Framework' (2004) 19(1) *Journal of Business and Psychology* 85; D Gefen, 'E-Commerce: The Roles of Familiarity and Trust' (2000) 28 *Omega* 725; TSH Teo and J Liu, 'Consumer Trust in E-Commerce in the United States, Singapore, and China' (2007) 35 *Omega* 22; PA Pavlou, 'Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model' (2003) 7(3) *International Journal of Electronic Commerce* 101; LV Casalo, C Flavian and M Guinaliu, 'The Influence of Satisfaction, Perceived Reputation and Trust on a Consumer's Commitment to a Website' (2007) 13(1) *Journal of Marketing Communications* 1; C Flavian, M Guinaliu and R Gurrea, 'The Role Played by Perceived Usability, Satisfaction, and Consumer Trust on Website Loyalty' (2006) 43 *Information & Management* 1; SJ Yoon, 'The Antecedents and Consequences of Trust in Online-Purchase Decisions' (2002) 16(2) *Journal of Interactive Marketing* 47; C Chen, 'Identifying Significant Factors Influencing Consumer Trust in an Online Travel Site' (2006) 8 *Information Technology and Tourism* 197; DJ Kim, DL Ferrin and HR Rao, 'A Study of the Effect of Consumer Trust on Consumer Expectations and Satisfaction: The Korean Experience' in *Proceedings of the 5th International Conference on Electronic Commerce* (ACM, 2003) 310; M Koufaris and W Hampton-Sosa, 'The Development of Initial Trust in an Online Company by New Customers' (2004) 41 *Information & Management* 377; DH McKnight, H Choudhoury and C Kacmar, 'The Impact of Initial Consumer Trust on Intentions to Transact with a Web Site: A Trust Building Model' (2002) 11 *Journal of Strategic Information Systems* 297.

25 F Bélanger and L Carter, 'Trust and Risk in E-Government Adoption' (2008) 17(2) *Journal of Strategic Information Systems* 166.

26 *Ibid*, 167.

27 Pavlou (n 25); Casalo, Flavian and Guinaliu (n 25); Flavian, Guinaliu and Gurrea (n 25); Yoon (n 25).

Ease of use of a particular website or web application appears to increase user trust.[28] This seems to be the case especially with users new to a particular electronic service. An inconvenient arrangement and complicated navigation appear to make the user unsure and anxious about technical mistakes.[29]

The *quality of the service* offered is of course also relevant to the creation and preservation of trust. *Advantages in terms of saving time and effort* in comparison to the traditional ways of providing the service involved can also offer important motives for trust. In the context of electronic services by the government, attributes such as helpfulness and simplification of complex tasks appear to increase the level of trust and user acceptance.[30]

Security of databases and communications is a quintessential precondition for trust in electronic services, including e-health services. While user trust is already considered essential for online commercial transactions,[31] building user trust in e-health services is deemed extra important as users may fear unwarranted access to sensitive personal information or vulnerability to identity theft or online fraud—risks that do not arise as easily in comparable traditional offline practices, at least not to the same degree.[32]

The factors mentioned so far have been shown to be important for users' trust in online services in general, and can therefore be expected to be important for patients' trust in e-health as well. In addition, for caregivers, trust in the *reliability of data, data exchange and communication* is reported to be of high importance.[33] Means for establishing reliability are of course to be found in the creation of possibilities for checking correctness and correction of information, for example through transparency and simplicity, and security safeguards in databases and communications. For health professionals, reliable authentication methods are also extremely important in order to guarantee that a patient is who she suggests she is and that the data introduced are really hers.

This brings us to data protection regulation as a precondition for user trust. According to the WHO report cited in the introduction, privacy and trust in a healthcare context are intrinsically linked. The relationship between the patient and the healthcare provider

28 Y Bart, V Shankar, F Sultan and GL Urban, 'Are the Drivers and Role of Online Trust the Same for All Web Sites and Consumers? A Large-Scale Exploratory Empirical Study' (2005) 69 *Journal of Marketing* 133.

29 Flavian, Guinaliu and Gurrea (n 25).

30 J Lee and HR Rao, 'Task Complexity and Different Decision Criteria for Online Service Acceptance: A Comparison of Two E-Government Compliance Service Domains' (2009) 47 *Decision Support Systems* 424.

31 OB Buttner and AS Göritz, 'Perceived Trustworthiness of Online Shops' (2008) 7 *Journal of Consumer Behavior* 35; A Everard and DR Galleta, 'How Presentation Flaws Affect Perceived Site Quality, Trust, and Intention to Purchase from an Online Store' (2005) 22(3) *Journal of Management Information Systems* 55; Gefen (n 25); Teo and Liu (n 25); McKnight, Choudhoury and Kacmar (n 25).

32 SE Colesca, 'Increasing E-Trust: A Solution to Minimize Risk in E-Government Adoption' (2009) 4(1) *Journal of Applied Quantitative Methods* 31.

33 AMC/NIVEL, 'Vertrouwen van zorgverleners in elektronische informatie-uitwisseling en het landelijk EPD. Een juridische en sociaal-wetenschappelijke studie naar de positie van zorgverleners' (Onderzoeksrapport afdelingen Sociale Geneeskunde & Klinische Informatiekunde, AMC/NIVEL 2011) 29–32.

is one based on trust, where the patient provides and shares different types of sensitive information about herself and trusts that the healthcare provider will use that information to the best of her interests in terms of help and treatment.[34] One should expect the willingness of users to provide their personal data to increase if they trust the healthcare providers involved and the system provider.[35] Willingness to disclose personal data may also increase when the user is of the opinion that the advantages of the transaction are more important than a higher level of privacy.[36]

Research into electronic services in other contexts suggests that the presence of privacy policy statements on a website enhances user trust.[37] Privacy policy statements, however, are rarely read.[38] Explicit indications that service providers intend to secure online transactions by means of technological measures, such as Privacy Enhancing Technologies (PETs) or authentication methods, were expected to increase the trust of new users.[39] However, Kool *et al*[40] were not able to find unambiguous support for this claim.

This leads to the question of whether the law can further contribute to the fulfilment of the conditions for trust in e-health outlined above.

V. THE LAW AS A FACILITATOR OF TRUST IN E-HEALTH

Some of the conditions that facilitate trust in e-health applications depicted in the preceding section, such as ease of use and advantages in terms of saving time and effort, are concerned with the specific design of a particular application, rather than with the

34 See n 1, n 37 and n 67.

35 F Bélanger, JS Hiller and WJ Smith, 'Trustworthiness in Electronic Commerce: The Role of Privacy, Security, and Site Attributes' (2002) 11 *Journal of Strategic Information Systems* 245; McKnight, Choudhoury and Kacmar (n 25).

36 B Berendt, O Gunther and S Spiekermann, 'Privacy in E-Commerce: Stated Preferences vs Actual Behaviour' (2005) 48 *Communications of the ACM* 101; PA Norberg and RR Dholakia, 'Customization, Information Provision and Choice: What Are We Willing to Give Up for Personal Service?' (2004) 21 *Telematics and Informatics* 143; MJ Culnan and RJ Bies, 'Consumer Privacy: Balancing Economic and Justice Considerations' (2003) 59(2) *Journal of Social Issues* 323; N Olivero and P Lunt, 'Privacy Versus Willingness to Disclose in E-Commerce Exchanges: The Effect of Risk Awareness on the Relative Role of Trust and Control' (2004) 25 *Journal of Economic Psychology* 243.

37 TW Lauer and X Deng, 'Building Online Trust through Privacy Practices' (2007) 6 *International Journal of Information Security* 323; DB Meinert, DK Peterson, JR Criswell and MD Crossland, 'Would Regulation of Website Privacy Policy Statements Increase Consumer Trust?' (2004) 9 *Informing Science Journal* 123; Y Pan and GM Zinkhan, 'Exploring the Impact of Online Privacy Disclosures on Consumer Trust' (2006) 83(4) *Journal of Retailing* 331.

38 M Arcand, J Nantel, M Arles-Dufour and A Vincent, 'The Impact of Reading a Website's Privacy Statement on Perceived Control over Privacy and Perceived Trust' (2007) 31(5) *Online Information Review* 661; Meinert *et al* (n 38).

39 Koufaris and Hampton-Sosa (n 25).

40 Kool *et al* (n 25).

context within which e-health is offered. Others, such as previous experience with an e-health application, healthcare provider, information technology developer or patient, and a user's propensity to trust the internet, are dependent mainly upon the character and the experiences of a particular user. For the other conditions—and in particular for establishing and preserving the reputations of key players and of e-health systems themselves, security of databases and communications, reliability of data, data exchange and communication—the law can play an important role in providing the framework for certainty and expectations on behaviour.

Privacy, the Duty of Confidentiality and Data Protection

Privacy protection aims at safeguarding human autonomy and reducing the vulnerability of individuals with regard to material harm and immaterial damage, such as discrimination or stigmatisation. Privacy also protects social values, as it enables citizens to form their own opinions and preferences, thus contributing to the diversity of ideas and fostering creativity in society. This is reflected in the respect required by law of an individual's privacy. Privacy is the right to be in control of one's personal sphere in its manifold spatial, relational and informational dimensions. It has been recognised as a human right at both the international and national levels. Article 12 of the Universal Declaration of Human Rights states that '[n]o one shall be subjected to arbitrary interferences with his privacy' and asks for the establishment of a right 'to the protection of the law against such interference or attacks'. In Europe, the European Convention on Human Rights stipulates in Article 8 that everyone has the right to 'respect for his private and family life, his home and his correspondence'.[41]

An important instrument for safeguarding patients' privacy and, indirectly, ensuring unhindered access to healthcare for all patients is the caregiver's duty to respect his patients' confidentiality.

The duty of confidentiality is the obligation of healthcare providers not to disclose personal sensitive information about patients to third parties.[42] As this duty is reinforced by legal obligations, healthcare providers' interests dictate that e-health systems protect the privacy of their clients and that the relevant responsibilities of various other stakeholders, such as the engineers who design the system, are accurately and transparently divided. The obligation on healthcare providers to keep certain information secret,

41 Art 8(1) European Convention on Human Rights. The Convention provides a jurisdiction, currently exercised by the European Court of Human Rights (ECHR) in Strasbourg, to which allegations that a Contracting State is not meeting one of its obligations can be brought.

42 In short, medical professionals' duty of confidentiality has to be taken into account when patient data is exchanged. The duty of confidentiality applies to all information about patients, including the information that someone is a patient of a healthcare provider. Several exceptions to the duty of confidentiality exist, such as the patient's consent or the direct involvement of medical professionals in a medical treatment agreement. Preferably, permission must be obtained from the patient involved, even if such a requirement may create practical difficulties.

backed up by liability mechanisms in case of a breach of this duty, has the potential to increase patients' trust in health services. Of course, the influence of liability mechanisms extends beyond responsibility for confidentiality, as the obligation of healthcare providers to give proper medical treatment concerns much more than legitimate processing of personal data. Therefore, in the latter part of this section, we will address the possible impact of liability law in establishing or increasing trust in e-health.

The significance of personal data protection and confidentiality is even greater in the context of e-health, where the handling of patient data and information is pivotal. Nonetheless, many questions still remain unanswered. As we move from the personal patient–doctor relationship to a more impersonal provision of healthcare where new players, such as system providers, are involved, the question arises as to whether these intermediaries who have access to patients' sensitive personal data should also bear a duty of confidentiality towards the patient. A legally enforceable obligation of confidentiality may ensure that the patient's trust, which currently resides in the physician, extends to a larger number of people and institutions involved in the provision of healthcare in the era of e-health, and may eventually lead to an inherent trust in e-health itself. In some jurisdictions, for example in the Member States of the European Union, system providers already bear obligations not to disclose patient data based on data protection norms.

As the provision of e-health services is largely based on the collection and processing of patients' sensitive data, trust in such services may be severely undermined if the personal data of users is mishandled. Whenever an individual is examined by a physician or is tested by medical devices, a vast amount of data is collected, such as name, gender, address and phone number, as well as information about the patient's health condition. The legislature has intervened, at least in Europe, to protect individuals against the illegitimate collection and processing of personal data by establishing strict data protection obligations.[43]

In 1995 a general Directive regarding the processing of personal data (DPD) was adopted in the European Union,[44] based upon the OECD privacy principles: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.[45] The DPD sets out the main rights and obligations to be respected when processing personal data. Besides provisions that apply to all processing of personal data, some provisions concern the processing of

43 At an international level the first initiatives to regulate data collection were taken in the 1980s by the Organisation for Economic Cooperation and Growth and the Council of Europe. Nonetheless, their success in creating homogeneous rules has been questioned. For the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, see www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

44 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.1995.

45 See: www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

so-called sensitive data, including data concerning health.[46] In principle, the processing of sensitive data is prohibited unless one of the grounds in Article 8(2) applies, meaning that in several instances sensitive data can only be processed when the data subject has given her consent. For health data an exception exists in Article 8(3), lifting the prohibition to process health data

> where processing of the data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

As we speak, in December 2014, the European legal framework for the protection of personal data is being reviewed.[47] A proposal is pending to replace the DPD with a regulation. The difference between directives and regulations is that directives need to be implemented within the national legal regimes of all EU Member States, while regulations are directly effective in all EU Member States without the need to implement them in national legal systems. To some extent the main provisions regarding processing health data in the regulation are quite similar to the fundamentals set out in the DPD. The regulation, however, adds some interesting details. To begin with, a definition of 'data concerning health' is provided, namely: 'Data designating information about physical or mental health of an individual or the provision of health services to the individual.'[48] Moreover, besides a provision resembling Article 8 of the DPD,[49] the proposed regulation contains Article 81, a provision specifically aimed at processing data concerning health.[50] Article 81 lists the purposes for which, in accordance with the rules set out in the regulation, data concerning health may be processed on the basis of Union law or Member State law. These purposes include preventive and occupational medicine, medical diagnosis, the provision of care and treatment, the management of healthcare services, and reasons of public interest in the areas of public health and social protection. Interestingly, it is added that, if the purposes[51] can be achieved without the use of personal data, such data shall not be used unless the data subject has given consent. Article

46 Art 8 DPD.

47 Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, COM(2012) 11/final, 25.01.2012. The references in this paper to provisions of the proposed regulation are based upon the text of the proposed regulation as adopted by the European Parliament (first reading) of 12 March 2014: www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN.

48 Art 4(12) of the proposed regulation.

49 Art 9 of the proposed regulation.

50 See also recital 42.

51 Referring to the purposes mentioned in points (a) to (c) of Art 81(1).

81 provides guidelines on how to consent to the processing of medical data for public health purposes, statistical and scientific research purposes and clinical trials.

The text of the proposed regulation as adopted by the European Parliament also contains a very interesting new recital 122a. It states:

> A professional who processes personal data concerning health should receive, if possible, anonymised or pseudonymised data, leaving the knowledge of the identity only to the General Practitioner or to the Specialist who has requested such data processing.

However, this recital is not incorporated in any of the provisions of the proposed regulation.

Compared to the DPD, the proposed regulation contains several unique features that will have an influence on the processing of health data, including Data Protection Impact Assessments and the principles of Privacy by Design and Privacy by Default. The proposed Article 32a obliges a controller, or where applicable a processor, to carry out a risk analysis when processing operations are likely to present specific risks. Several processing operations are indicated as being likely to present specific risks, including the processing of sensitive data, and more specifically the processing of personal data for the provision of healthcare, epidemiological researches, and surveys of mental or infectious diseases, where the data are processed for taking measures or decisions regarding specific individuals on a large scale. If the risk analysis warrants this, the controller or the processor acting on the controller's behalf will carry out a data protection impact assessment, as prescribed in Article 33. Such an assessment will concern the impact of the envisaged processing operations on the rights and freedoms of the data subjects, especially their right to protection of personal data. The results of the impact assessment must be taken into account when developing measures and procedures aimed at complying with the principles of Privacy by Design and Default. These principles are defined in Article 23 of the proposed regulation:

> [B]oth at the time of the determination of the purposes and means for processing and at the time of the processing itself, appropriate and proportionate technical and organisational measures and procedures must be implemented in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject … Data protection by design shall have particular regard to the entire lifecycle management of personal data from collection to processing to deletion, systematically focusing on comprehensive procedural safeguards regarding the accuracy, confidentiality, integrity, physical security and deletion of personal data.

As the specifics regarding if, when and how the proposed regulation will be adopted are not yet certain,[52] now is not the time to undertake an in-depth analysis of the influences

52 C Kuner, *The European Commission's Proposed Data Protection Regulation: A Copernican Revolution in European Data Protection Law*, Bloomberg BNA Privacy and Security Law Report, 6 February 2012, pp

of the regulation on trust in e-health. However, the above clearly demonstrates that the new legal regime will be of importance to trust in e-health. It provides a framework on the basis of which all parties involved in the processing of personal data must obey the general rule that data may only be processed fairly and lawfully, meaning that all obligations deriving from the European legal framework regarding data protection must be complied with.

Other jurisdictions, such as the United States, do not have one comprehensive legal framework on privacy and data protection. Although the right to privacy is not explicitly mentioned in the US Constitution, it has been inferred and recognised in several amendments, such as freedom of thought (1st amendment) and protection from unreasonable searches (4th amendment).[53] Being a federal country, powers that have not been delegated to the US Federal Government are reserved to the states respectively. In addition, the US has various pieces of legislation at the federal level protecting the right to privacy in specific domains or regarding a particular area of privacy. Among these are the Freedom of Information Act of 1966, which allows access to most federal government records by any citizen, and the Privacy Act of 1974, which provides citizens with safeguards with regard to the misuse of personal information records of federal agencies.

Specifically with regard to medical records, it is worth mentioning the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[54] HIPAA includes a set of specific rules that envisage the federal protection of individually identifiable health information, provides patients with a set of rights regarding that information, and establishes specific mechanisms to be followed in case of a breach of unsecured protected health information. The HIPAA rules apply to individuals, organisations and agencies, referred to as 'covered entities', such as healthcare providers, health plans and health clearinghouses, which transmit health information in electronic form in connection with transactions covered by the rules. The rules also apply to covered entities' business associates.[55] In particular, the HIPAA privacy rule provides a set of standards which aim at protecting 'individually identifiable health information', to be applied nationwide by organisations subject to this privacy rule. In addition, the HIPAA privacy rule provides standards for the exercise of individuals' privacy rights in relation to their health information (in oral, written and/or electronic format). To complement this, the HIPAA

1–15: http://ssrn.com/abstract=2162781; C Cuijpers, E Kosta and N Purtova, 'Data Protection Reform and the Internet: The Draft Data Protection Regulation' in A Savin, and J Trzaskowski (eds), *Research Handbook on EU Internet Law* (Edward Elgar, forthcoming).

53 For examples of specific rulings of the US Supreme Court on the right of privacy, see www.supremecourt.gov/default.aspx.

54 Further information on the HIPAA Privacy, Security and Breach Notification Rules can be found at the US Department of Health & Human Services website: www.hhs.gov/ocr/privacy/index.html.

55 The HIPAA refers to 'business associate' in relation to those persons or organisations who collaborate with cover entities in performing certain activities which involve using or disclosing protected health information. It is envisaged that a specific agreement needs to be settled between cover entities and business associates guaranteeing that the latter will comply with HIPAA Rules.

provides the security rule, which obliges covered entities to implement security standards in order to protect the privacy, security and exchange of health information kept in electronic format. The Office for Civil Rights (OCR) of the US Department of Health and Human Services is the organisation responsible for the enforcement of and compliance with the HIPAA rules by the covered entities. In addition, the HIPAA provides a breach notification rule where unsecured protected information is breached by covered entities and their business associates.[56] In this sense these parties need to notify the individuals and the Department of Health and Human Services—and in some specific cases even the media—about any breach. Moreover, the Department of Health and Human Services is required to publicise the list of entities that have experienced breaches of unsecured protected health data. Finally, the HIPAA rules also empower the individual with specific options for filing complaints where there has been a violation of HIPAA.

While HIPAA has been the object of critical descriptions, ranging from 'toothless' to 'over-burdensome', after 10 years of HIPAA, Solove concludes that it has evolved over the years and that it has been shown to have a vast impact on patients, medical professionals and the healthcare industry.[57] A particularly notable development was the Health Information Technology for Economic and Clinical Health (HITECH) Act, which strengthened HIPAA by dramatically increasing the penalties for HIPAA violations and making it directly applicable to business associates. In the HITECH Act the federal government's goal of achieving interoperability by building a nationwide health information technology infrastructure that permits the electronic exchange and use of health information is legally anchored.[58] In January 2013, the Department of Health and Human Services (HHS) issued the final regulation implementing the HITECH's Act HIPAA modifications. Solove concludes his analysis of HIPAA as follows:

> With the increased enforcement and auditing, as well as its increased scope, HIPAA is a force to be reckoned with. It has come out of the last decade stronger and more influential. And its influence will surely grow.[59]

56 On 14 February 2014, in a lecture accepting the appointment of professor of Global ICT Law at Tilburg University, L Moerel observed that when drafting the proposed regulation the European Commission kept the EU system and adopted on top of that parts of the US system that have proven effective in practice, amongst them the Data Breach Notification and Arts 31 and 32 of the proposed Regulation: www.debrauw.com/wp-content/uploads/NEWS%20-%20PUBLICATIONS/Moerel oratie.pdf.

57 DJ Solove, 'HIPAA Turns 10: Analyzing the Past, Present, and Future Impact' (2013) 84 *Journal of AHIMA* 23. (The act was passed in 1996, but took effect in 2003.)

58 American Recovery and Reinvestment Act of 2009, Pub L No 111-5, § 3002(b)(1), 123 Stat 115, 234 (2009) (to be codified at 42 USC § 300jj–12(b)(1)).

59 (n 58) 28.

Responsibility and Liability

Unlike the legal regimes concerning privacy and data protection, the EU and US regimes regarding liability for medical malpractice are similar to each other. Medical malpractice is defined as any act or omission by a care provider during treatment of a patient that deviates from accepted norms of practice in the medical community and causes an injury to the patient.[60] In relation to the provision of e-health services it is important to stress that other parties might be responsible for providing improper care, perhaps because of malfunctioning hardware or software used to provide the e-health service. However, from the perspective of the patient this is part of the treatment given by the care provider, and thus, for the patient, the care provider is the first port of call in case of injury during treatment.

There is no EU legal framework regarding medical malpractice. While some elements can be traced back to EU directives, in general national laws govern medical malpractice in the EU.[61] Likewise, in the US there is no overarching substantive federal law governing medical malpractice. There, medical malpractice law falls under the authority of the individual states; the framework and rules that govern it have been established through decisions of lawsuits filed in state courts. Thus, state law governing medical malpractice can vary across different jurisdictions in the US, although the principles are similar.[62]

There are also many similarities between the EU and US systems in terms of content, at least on a general level, although details can differ in specific (member) state legislations. While private contracts are usually concluded at the beginning of a treatment, it is the factual situation of a person in need of treatment being accepted for treatment by another person that brings about the care provider–patient relationship. In general, the care institution is vicariously liable for its employees when they act in the course of their employment. In both the EU and the US, fault, or at least negligence, is required for liability, as well as causation between the patient's injury and the care provider's negligence. In principle, the patient must prove both negligence and causation. Whether or not a care provider acted negligently is assessed on the basis of the average standard of care, meaning: 'A physician or other medical service provider must act with such reasonable skill and care which an ordinarily careful specialist of the same profession under same circumstances would be expected and required to exercise.'[63] This duty, in both the EU and the US, extends to the supervision and control of technical applications and/

60 BS Bal, 'An Introduction to Medical Malpractice in the United States' (2009), www.ncbi.nlm.nih.gov/pmc/articles/PMC2628513.

61 To give an example, the rules on unfair terms in consumer contracts, as laid down in Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, OJ L95, 21.4.1993, pp 29–34, also apply to medical treatment contracts.

62 See above, n 61.

63 U Magnus and HW Micklitz, 'Comparative Analysis of National Liability Systems for Remedying Damage Caused by Defective Consumer Services, Part D: The Comparative Part' (2004), http://ec.europa.eu/consumers/cons_safe/serv_safe/liability/reportd_en.pdf.

or services. Another important similarity concerns the obligation to properly inform patients about all relevant aspects of the illness and treatment.

While, overall, malpractice regulations are similar in the EU and the US, one important difference concerns the amount of malpractice lawsuits, being way higher in the US than is the case in the EU. The reason for this, however, is not the malpractice legislation itself but rather the unique claim culture as a consequence of the US judicial system.[64]

Although the effect of malpractice lawsuits on the quality of healthcare is hotly contested, a recent study showed that

> Hospitals, once afraid of disclosing and discussing error for fear of liability, increasingly encourage transparency with patients and medical staff. Moreover, lawsuits play a productive role in hospital patient safety efforts by revealing valuable information about weaknesses in hospital policies, practices, providers, and administration.[65]

The key in the argument seems to be transparency, generally hailed by many as the key to trust in other domains where digitisation has changed the traditional landscape, such as e-government.[66] A similar correlation between liability, transparency and trust can be expected in the domain of e-health. As described in section III, e-health systems fundamentally change the traditional healthcare domain. In view of this, a re-evaluation of applicable liability laws in the e-health domain is required, as, for several reasons, the allocation of responsibilities is more complicated.

First, e-health is based on increasingly complex interactions, which augment the difficulties of proving causation. Demonstrating and assessing causation between medical fault and injury is already complex in traditional cases of medical malpractice;[67] it gets even more complicated in e-health as multiple actors are involved in the treatment of a patient and damage can be the result of a multitude of factors.[68] The increasing involvement of patients themselves in their own treatment, combined with the provision of care by multiple physicians and other care providers, as well as the role of providers of care technologies, creates uncertainty as to causation in case of injury or other harm to the patient. For instance, who is responsible for damage caused to the patient where a third person has, for instance, measured her blood pressure and passed the result on to a care provider attributing the data to the patient, without the patient being aware? In such cases the law needs to determine the conditions under which health-

64 AL Sorrel, 'Medical Liability: A World of Difference' (2010), www.amednews.com/article/20100503/profession/305039938/4.

65 JCA Schwartz, 'A Dose of Reality for Medical Malpractice Reform' (2013) 88 *NYU Law Review* 1224; UCLA School of Law Research Paper No 13-37, http://ssrn.com/abstract=2104964.

66 S Grimmelikhuijsen, 'Linking Transparency, Knowledge and Citizen Trust in Government: An Experiment' (2012) 78(1) *International Review of Administrative Sciences* 50, http://ras.sagepub.com/content/78/1/50.full.pdf+html.

67 L Khoury, *Uncertain Causation in Medical Liability* (Hart Publishing, 2006).

68 RW Wright, 'Causation in Tort Law' (1985) 73 *California Law Review* 1735.

care providers can plead the contributory fault of the claimant/patient as a defence or in diminution of damages. Moreover, because of the possibilities of using information and communication technologies to perform remote treatments without face-to-face contact, interference by malicious third parties (hackers) becomes a scenario to take into consideration. In the end, adapting and fine-tuning the liability rules might not be enough to solve all the difficulties related to the increase and change of actors and tools involved in medical treatment and the evidence of causation if damage occurs. As can be witnessed in the ObamaCare debate, reform of the healthcare system impacts not only insurance schemes but also the legal framework for medical malpractice.[69] Put differently, there is a close connection between insurance schemes and liability frameworks, which are heavily influenced by national context.[70] It is beyond the scope of this paper to discuss how the interrelation between liability and insurance can indeed solve issues like evidence of causation. It cannot be over-emphasised, however, that insurance can play a role here. As Ruger puts it: 'When individuals lack access to means of reducing or mitigating risks, they become insecure. Vulnerability and insecurity diminish well-being and inhibit human flourishing.'[71] From this perspective insurance could be considered as a trust enhancer. However, as already indicated, the correlation between malpractice law and medical insurance raises many specific legal questions in need of much wider and deeper legal analysis, which goes beyond the scope of this paper.

We continue our analysis of how e-health systems fundamentally change the traditional healthcare domain by indicating a second issue: as e-health constitutes a rather new technological development, there is still much to be explored from an evidentiary point of view. Law professionals, judges, physicians, patients and manufacturers still need to better understand and handle the real value and weight of e-health information evidence. Due to its characteristics, it might be difficult to prove in front of a court of law that the developers of an e-health system or the healthcare providers overseeing the application of a system were aware of the damage that the system might cause to a patient. This could lead to two scenarios. The courts and the legislature might impose too harsh obligations on physicians and e-health system providers acting in good faith, thus discouraging their further involvement in the provision of e-health, or the legal system might allow certain liability exemptions for actions for which they would have been held liable otherwise, thus undermining patients' trust in e-health.

69 See in this respect eg Alexander C Davis, 'The Impact of the Affordable Care Act on Medical Malpractice Litigation' (30 April 2012), http://ssrn.com/abstract=2048561; Richard A Epstein and David A Hyman, 'Fixing Obamacare: The Virtues of Choice, Competition and Deregulation' (2013) 68 *NYU Annual Survey of American Law* 493; University of Chicago Law & Economics, Olin Working Paper No 418; University of Illinois Law & Economics Research Paper No LE08-023, http://ssrn.com/abstract=1158547.

70 For a comparative analysis of national healthcare systems see Michael Tanner, 'The Grass is Not Always Greener: A Look at National Health Care Systems around the World' (18 March 2008), Cato Policy Analysis Paper No 613, http://ssrn.com/abstract=1262978.

71 Jennifer Prah Ruger, 'The Moral Foundations of Health Insurance' (2007) 100 *Quarterly Journal of Medicine* 53, 54, http://ssrn.com/abstract=957971.

Third, the increased contribution of the patient in her treatment raises questions regarding the patient's duties and responsibilities to make use of the e-health system in good faith. Especially with regard to e-health applications that require considerable discipline and frequent and regular exercises or, for instance, taking blood pressure or testing by the patient, it is not hard to imagine scenarios where patients might skip their exercises, mislead the system or feed it with incorrect data, or even let others provide data—simply because they are unable to follow or live up to the regime.[72] Some might even try to take advantage of the e-health system and the lack of physical presence of a physician in order to defraud their insurance company. As the patient is assigned an active role in examining her condition, reporting the resulting data and administering her own treatment, it is only natural that she should share the responsibilities, if only for motivational reasons. Of course, this important new feature of e-health confronts us with important ethical questions regarding an individual's responsibility for her own health. These questions do not merely extend to the potential psychological burdens of the patient; they also impact on stimulating movements towards 'medical self-management', which may have both positive and negative effects for the sustainability of the healthcare system.[73]

The imposition of harsh or lenient obligations on hospitals, electronics and software manufacturers, physicians and patients can influence trust in and the acceptance of e-health systems in diverse ways and can create conflicting incentives for the adoption of e-health services. On the one hand, the imposition of strict obligations for healthcare providers, funding bodies and electronics and software manufacturers is likely to strengthen patient trust in e-health. On the other hand, the fear of liability might simultaneously prevent care providers from adopting e-health applications. In this sense, liability laws carry with them a dissuasive or chilling effect for those who have to decide whether or not to undertake certain activities, since all activities could trigger liability.[74] However, in the early stages of the development of new technologies, such as e-health systems, experimentation and risk-taking may be desirable, as they can lead to advancements in the existing technological state of the art.[75]

The law should strive to strike a careful balance between the conflicting interests of patients and healthcare providers, so as to protect patients' health and encourage user trust in e-health systems, while at the same time encouraging innovation, technological development and investment in the provision of e-health services.[76]

72 Issues regarding access to data, confidentiality of data and the processing of personal and sensitive data are not discussed here as they have been addressed in section IV.

73 A Vedder, 'Will Technology Save the Health Care System?' in R Leenes and E Kosta (eds), *TILTing Perspectives 2013: Bridging Distances in Technology and Regulation* (Wolf Legal Publishers, 2013).

74 JEJ Prins and MHM Schellekens, 'The Chilling-Effect of Liability Law on Initiatives to Enhance the Reliability of On-Line Health-Related Information' (2004) 11(2) *European Journal of Health Law* 204.

75 EM Salzberger (ed), *Law and Economics of Innovation* (Edward Elgar, 2012).

76 K McClanahan, 'Balancing Good Intentions: Protecting the Privacy of Electronic Health Information' (2008) 28(1) *Bulletin of Science, Technology & Society* 69; MA Rothstein, 'The Hippocratic Bargain and Health Information Technology' (2010) 38(1) *Journal of Law, Medicine & Ethics* 7.

VI. CONCLUSION

Trust is an important precondition for the adoption of new technologies. User trust is vital in the case of electronic services, such as e-health, for which very often traditional alternatives are still available. Raising or at least preserving trust, in addition to efficacy, efficiency and safety, may be necessary to persuade people to start using and keep using electronic alternatives.

Technology, law and trust interact and influence each other. E-health shifts the roles of patients and care providers, creates and incorporates a new role for system providers, and changes the relationships among these groups. This shift impacts upon trust in technology and trust among the actors, on the one hand, and leads to a change in the actual division of ethical and legal responsibilities of patients, care and system providers, on the other. By anticipating, accompanying and providing responses to the changes brought about by e-health systems, law can strengthen trust in e-health services and thus facilitate its adoption. Of course, law can also play a direct role in the development of technology. Here, one can think of the prescribed use of technology or built-in technological mechanisms to respect data protection regulations in e-health systems. Technological solutions, such as video chat, means for checking correctness and correction, privacy policy statements embedded in websites, and PETs and privacy by design may also help to foster and strengthen user trust in e-health.

First and foremost, the likelihood of users being confronted with problems and adverse effects which they would not have met had they used the traditional facilities needs to be reduced and prevented. This article has identified and discussed the potential of law as an important factor in engendering trust in e-health: it can act as a safeguard for the prevention of harms, hazards and liabilities, provided that it is adapted in smart ways to the specific characteristics and challenges of e-health. The relevant stakeholders in the field, be they patients, healthcare providers or engineers, should be aware of this positive role of the law, in order for this potential to be realised. If full realisation must wait until there is a privacy violation, mishandling of personal data, patients' misrepresentation of their condition, or other medical malpractice or system malfunction invoking law enforcement mechanisms, it may be too late. In that case, the law will be acting *ex post*, and real events may already have jeopardised trust in e-health. Still, also in these *ex post* situations, legal frameworks may help to restore trust, for example when liability regimes properly provide for compensatory damages where harm has been suffered.